Contact

For support, service and repair please contact:

e-mail: support@cryptophone.de

phone: +49 700 CRYPTTEL

fax: +49 700 CRYPTFAX

Further information: http://www.cryptophone.com

© 2005
Gesellschaft für Sichere Mobile Kommunikation mbH
(GSMK), Berlin, Germany

GSMK CryptoPhone G10 User Manual

General	3
Inserting SIM card & switching the phone on	3
Enter your PIN	4
Charging	4
Standby	6
Flight Mode	6
Placing an Encrypted Call	7
Key Verification	8
Call Quality during Secure Calls	9
Switching the Calltype	10
Problems with setting up a Secure Call	11
Changing the volume	13
Mute during call	14
Secure Push to Talk	14
Secure Calls while moving	15
Redialing	16
Calling from the Contacts list	16
General Mobile Phone Security Advice	17
Power down	17
Cold Boot & Emergency Erase	17
Security Advice regarding Flash Memory	19
Using the headset	20
Bluetooth headset	20
Sync Contacts and Appointments	21
Troubleshooting	22
Security Updates	22
Security, Storage and Handling	24
Repairs	25
Accessories	26
3rd Party Software	27
Contact	28

3rd Party Software

In theory it is possible to install Microsoft Smartphone compatible 3rd party software on your GSMK CryptoPhone device. You should know that 3rd party software of any kind can be used to attack the integrity and security of your GSMK CryptoPhone. Installing additional software on Communication Security equipment like the CryptoPhone is a grave security risk that you should only take if it is absolutely necessary. Please be aware that installing 3rd party software might irrevocably compromise the security of your CryptoPhone or damage its functionality.

GSMK does not provide any support for installing 3rd party software and will not provide support for problems caused by installing 3rd party software. Any and all problems caused by 3rd party software are not covered by warranty or support.

You have been warned.

If you require large number of custom CryptoPhones that include certain software components of your choice by default, please contact sales@cryptophone.de to discuss your requirements.

There is no such thing as a »restocked«, »refurbished« or »second hand« CryptoPhone. All sales are final. If your CryptoPhone is defective, we will either repair it or swap the electronics for a new factory fresh device. No parts that have been in the hands of other customers will be used in repairs. If you need a repair, please mail us at service@cryptophone.de, so we can instruct you about the proper shipping and security procedures. Shipments that arrive for repair without prior acknowledgment and/or in ignorance of the advised shipping method and security precautions will be ignored. Please understand that it is in your own interest to adhere to the security measures, since only this will enable us to fulfill your security requirements. Note: the high-power Lithium-Polymer rechargeable battery of the CryptoPhone is a wear-and-tear part and not covered by the warranty. Replacement batteries are available in normal PDA or mobile phone stores.

Accessories

The GSMK CryptoPhone is based on a device manufactured by HTC, sold under different brand names. Additional accessories for your CryptoPhone (like holsters, car kits, external antennas etc.) can therefore be easily obtained by buying kit that is destined for SDA, i-mate SP3i or Qtek 8020 devices.

General

Your CryptoPhone G10 is based on a generic tri-band (900/1800/1900) GSM Smartphone that is sold under different brand names. The phones firmware and operating system have been modified to accommodate the CryptoPhone functionality and provide added security, so a number of things that you might know from other Smartphones are not available on the GSMK CryptoPhone for security reasons. We supply the original Smartphone manuals, license sticker and CD with the GSMK CryptoPhone G10, but you need to be aware that some functionality has been disabled by us for security reasons. Do not try to use Microsoft operating system updates as this may destroy the CryptoPhone firmware and void your warranty. Certified CryptoPhone Updates are only provided by GSMK to you in a cryptographically secure manner.

Inserting SIM card & switching the phone on

You need to insert a valid GSM card (SIM) in the GSMK CryptoPhone G10 in order to place calls. To insert the SIM, remove the back cover of the device by pressing the latch on the lower backside and sliding the cover downwards. You will see the SIM card slot in the lower corner of the device. Lift up the SIM card cover

by pushing it in the direction marked “Open” and insert the SIM. Then click the SIM card cover down so that it is firmly closed. Now insert the battery (which is stored stored separately in the shipping box).

Replace the back cover by sliding it gently upwards onto the device. Now push the power button on the top of the device. The screen will light up and the GSMK CryptoPhone G10 begins its firmware initialization. This may take up to two minutes.

Enter your PIN

Most GSM SIM cards require you to enter a PIN number. After you have switched on the CryptoPhone, you will be asked to enter your PIN. After you entered the PIN, press the “Done” button. The CryptoPhone will finish initialization and provide the secure telephony mode. If your GSM SIM does not require a PIN, the secure telephony mode will be enabled right away. We recommend that a PIN number is used to enhance individual security.

Charging

Before using your CryptoPhone, we recommend that you charge the battery until full. In order to do this, you must connect the power supply to the CryptoPhone. Depending on your location, you may need a plug

sive scientific effort (several months of analysis at the cost of several 100.000 Euros per device). If in doubt and your security depends on it, consider purchasing a fresh unit.

The CryptoPhone is specified and designed for use in normal business, home and other general conditions. It is not reinforced or specially sealed against water and other harsh environmental conditions. (For reinforced versions of the CryptoPhone that comply with military specifications, contact us at sales@cryptophone.de). Submitting the CryptoPhone to excessively high or low temperatures (like in the outside pocket of an overcoat in cold climates) might temporarily or permanently damage the display and lead to accelerated battery aging, affecting the ability of the battery to store power and thereby reducing the standby time of your CryptoPhone. Sitting on the CryptoPhone or submitting the device to other heavy mechanical loads may damage parts of the phone, especially the keyboard. Damage to the keyboard, battery and display as well as any kind of other mechanical damage is not covered by the warranty.

Repairs

Because of the manipulation risk, we do not take back any CryptoPhones from customers, except for repairs.

immediately, as this may be an attempt to insert malicious firmware into your CryptoPhone. Please see our Questions and Answers section (Q&A) on the website http://www.cryptophone.com/ for further detailed information on the benefits of published source cryptography.

Security, Storage and Handling

Your CryptoPhone is a Communication Security (COMSEC) device. It can only be regarded as secure as long as you have permanent and uninterrupted physical control over the CryptoPhone. Once an adversary could have gained temporary physical possession of the CryptoPhone, it must be regarded as compromised. There is a variety of potential methods that would allow an adversary to listen into your calls after he manipulated the CryptoPhone and gave it back to you. Keep the handset with you securely at all times. Optimally, you should take it with you to the bathroom, put it beside your bed when you sleep and not leave it alone in the hotel room.

If you have »lost« the CryptoPhone and »find« it back again, it has to be regarded as compromised. Never lend your CryptoPhone. Major intelligence agencies are known for a wide variety of high-tech manipulation methods that are impossible to detect without a mas-

adaptor to use the power supply if the plug does not fit in your outlet. The power supply is rated 100-240V, which means it will accept your line voltage without conversion as long as it lies within this range. The LED in the upper area of your CryptoPhone will change color to yellow while the device is being charged, and to green when fully charged. You can either charge the CryptoPhone with the power supply (recommended) or with the supplied USB sync cable on a computer. Charging over USB takes considerably more time and is dependent on your computers configuration and setup, so it may not work under some circumstances (e.g. if you have no synchronization software installed on your computer or the USB port is not powered up).

Due to the higher power consumption of the built-in powerful computer and the backlit display, the standby and talk times in secure mode are less than what you might expect in normal GSM phones. Also please note that the standby and talk times may vary depending on your distance to the nearest GSM base station: the further away the base station, the more power your phone needs to use to reach it. Spare batteries are available in normal electronic stores that sell mobile phones.

Note: we recommend to charge your GSMK CryptoPhone every night or have a charged spare battery ready. For security reasons explained later in the chap-

ter 'Security, Storage and Handling', we suggest you keep the CryptoPhone with you at all times so that it is under your permanent supervision. If the phone rings or you need to place a call while the phone is charging, you can leave it plugged in while operating the phone.

Standby

The GSMK CryptoPhone has four basic modes of operation. It can be either completely switched off, in 'standby mode', active, or in 'flight mode'. In normal operation the CryptoPhone is in 'standby mode'. In standby mode, you can switch the device on at any time by briefly pressing the left button right below the display and disabling the key lock.

Now the screen will light up. To put the GSMK CryptoPhone G10 back in standby mode, simply wait until the the screen goes dark. The GSMK CryptoPhone will still receive incoming calls when it is in Standby mode. In other words: standby mode will not disable the radio.

Flight Mode

It is not safe to enter an airplane, hospital or other no-phone area with the GSMK CryptoPhone switched on or in standby mode. To ensure the radio is off, you need to enter 'flight mode'. To enter flight mode, press the On/Off button briefly and select "Flight Mode" in

new attack methods. Since the CryptoPhone comes with full published source code, the chances are much higher for a flaw to be discovered and fixed quickly than with any closed-source cryptographic product. Our advisory board of distinguished cryptographers and security researchers help us to identify and counter potential threats based on their intimate knowledge of the latest academic research and emerging cryptanalysis methods. In case a firmware update is needed for security reasons, you will get notified either via the e-mail address that you supplied when purchasing the CryptoPhone online, or directly by the distributor.

If you receive a notice about an upcoming security update, please verify it directly at our website http://www.cryptophone.com/ to prevent attackers from slipping you a malicious »update«. Please note that we will describe the details of the update procedure directly on the website.

The firmware update mechanism is cryptographically secured using a 4096 bit public key signature system, which ensures only signed CryptoPhone updates will be accepted by your CryptoPhone.

If you receive suspicious communication regarding CryptoPhone updates (such as an unannounced e-mail with an update file as attachment), please inform us

Troubleshooting

In the event that the Cryptophone reacts unexpectedly i.e., device response becomes very slow, key-lock can not be unlocked, or the phone does not connect to a GSM network, you can quickly reset it by removing and re-inserting the battery. The GSMK CryptoPhone will restart without erasing the memory. In the unlikely event such a problem persists, you can Cold Boot the device (see page 16). This will however delete all information in volatile memory.

Security Updates

GSMK continually seeks to improve the security and quality of operation of the Cryptophone G10. In the event anyone discovers a flaw in the CryptoPhone, we will provide a firmware update, as well as a detailed report on the possible security impact. As bad as security problems with cryptographic products can be, we believe the only way to handle them properly is open and transparent communication with our customers. You are the one best suited to determine potential damage to your interests, so we will provide you with all the known facts.

Security is not a state but a process. And this process requires constant checking against emerging risks and

the list by pressing the 2 key. You will now see a little x next to the antenna symbol when flight mode is active and the GSM is switched off. To switch the radio back on again, follow the same procedure and select “Flight Mode Off”. You will be required to enter your PIN again.

Placing an Encrypted Call

In order to place a secure call, the following conditions need to be met:

- your partner has a CryptoPhone compatible device up and running
- there is sufficient GSM coverage
- the GSM operator supports ‘GSM data calls’ (technically called Circuit Switched Data or ‘CSD’)

To place a secure call, you can simply dial from the home screen and press the “Call Secure” softkey on the left side. Also you can choose “Contacts”, select a contact and press “Call Secure”. Further you can switch to the CryptoPhone screen by pressing the home key and dial directly (press the green Call button after entering the number.

You will hear a bit of comfort noise in the speaker, followed by the normal ringing tone. It may take a bit longer than normal before the connection is made, so please let it ring. After your partner has pressed the Talk button on his end, you will hear a ditt-dutt ditt-dutt sound that signals to you that the 'key setup' procedure for the secure connection is in progress. Key setup may take from 3 to 30 seconds, but typically 8 seconds, depending on line quality. Once key setup is completed you hear a »Ping« sound and can start talking to your partner. In order to verify the authenticity of the key, Please take a look at the display and read the three letters under »you say« to your partner and verify the three letters under »partner says«. The green SECURE indicator is only visible when a secure call is established. During all other times it is shown in grey with a open lock.

Key Verification

Reading the three letters and verifying what your partner says is meant to protect you against so-called 'man-in-the-middle attacks' on the secret session key. The letters are mathematically derived from the unique secret key that is used during each call. By reading and

Sync Contacts and Appointments

The CryptoPhone supports in principle the sync of contact and calendar entries with a computer. You need to be aware that in theory it might be possible to attack the operating system of the CryptoPhone by supplying manipulated data to your PC or exploiting unknown problems in ActiveSync. GSMK does not recommend to sync your CryptoPhone with a PC, especially if the PC is connected to a network, for security reasons. If you have high security demands and need to calculate with a very sophisticated adversary, avoid to sync your CryptoPhone with a PC. The CryptoPhone ships with de-activated Active Sync functionality. You need to re-activate the sync option manually in the CryptoPhone to use it. To initiate a sync, connect the CryptoPhone with the computer using the enclosed USB cable.

Note: Sync over IrDa (Infrared) and Bluetooth has been disabled on the CryptoPhone as a precautionary security measure. While we are currently not aware of actual problems with these sync options, there is a very strong likelihood that such problems will arise in the future. The main risk is that an adversary could potentially gain wireless access to your device while it is in your pocket or just on the desk in front of you.

Using the headset

For hands free operation, a stereo headset is included with the GSMK CryptoPhone. You can plug it in any time, before or during a call, however you may terminate an ongoing call under some conditions when inserting the headset plug off-angle. The headset cable connector socket is on the lower right side of the device. GSMK does not provide support for problems caused by using headsets other than the one supplied with your CryptoPhone.

Bluetooth headset

The CryptoPhone G10 has a Bluetooth interface. While it is possible to use a Bluetooth headset for making normal unencrypted phone calls, we strongly not recommend using a bluetooth headset during encrypted calls. The reason is that with a Bluetooth headset you would broadcast the contents of your confidential calls before they have reached the encryption engine in the CryptoPhone. Bluetooth radio signals can be received over several hundred meters with moderately sophisticated equipment, so an attacker could listen to your calls easily. The encryption used with Bluetooth is no hurdle for a determined adversary and does not offer sufficient protection. We recommend using a wire based headset when placing secure calls.

verifying them with your partner, you make sure that you are indeed communicating using the same key. Please pay attention to the voice of your partner when he reads his three letters. To be completely on the safe side against very sophisticated voice impersonation during the key verification, you could periodically reverify the letter code with your partner during the conversation.

Call Quality during Secure Calls

The call delay indicator changes color in five steps between green over yellow to red. Green indicates the best call quality, red the worst. Delay describes the period of time it takes for your voice to reach your partner. This time gets longer if the transmission of the encrypted voice over the telephone network takes longer, or transmission errors occur.

Reasons for longer than normal delay are usually either bad GSM coverage or network congestion. Network congestion can often be circumvented by setting up the call again, sometimes you just get a »bad line«. The GSM data call mode, used by the CryptoPhone to transport the encrypted voice data during a call, has a certain delay, caused by the architecture of the GSM network. The GSM network handles data with lower priority than voice transmissions.

So even if the delay indicator is green, there is always a certain noticeable delay, much like on some transcontinental phone calls. If the overall line quality becomes bad, the delay rises and you may experience »drop outs«. Note that the quality on international calls might not be as good as on domestic calls. The multiple operators involved in an international call often try to minimize their costs by technical measures that can affect the quality of the call. If the call quality is unacceptable, please try calling again. Call quality can also be adversely affected when using certain GSM providers.

If the Delay indicator becomes reddish or red, please try to find a place with better GSM coverage. Use the signal strength indicator on the right upper side of the display to find a better spot. If the delay indicator turns and stays solid red, please hang up and set up the call again. When no call is in progress, the delay indicator is shown grey.

Switching the Calltype

Normally, the CryptoPhone uses the V.110 circuit switched data (CSD) - also called digital data call - bearer type to establish a secure connection. To call to an analog landline or to a CryptoPhone on a satellite network or a network with weird data-call configuration

Security Advice regarding Flash Memory

With the GSMK CryptoPhone, various information is stored in Flash Memory. Flash type storage is safe against failure of the backup-battery. You must however be aware that there is no way to securely erase information stored in flash memory in a way that it cannot be possibly reconstructed by sophisticated methods of computer forensics. Even if you erase the information and overwrite it with other data, it cannot be considered safely destroyed when stored on Flash Memory. Flash memory uses its own way of managing files that is beyond the control of the operating system.

So files that are no longer visible after deletion in the file manager may still exist in some unused part of the Flash memory. In addition, esoteric physical effects (" memory burn in ") make it possible for a forensic intelligence laboratory to reconstruct the former content of Flash memory, even if it has been erased or overwritten once. The same problem holds true for (mini)SD memory cards, because they are also based on flash memory technology. We therefore recommend that any potentially compromising information is not stored in the Flash Storage if there is a risk that the device may fall into the wrong hands.

sary. Cold Boot will not erase the contacts and SMS messages stored on your SIM card. Also, a Cold Boot does not erase any information that you may have stored in Flash (Storage) or on SD memory cards.

To initiate a Cold Boot follow the following procedure:,

1. remove the battery, re-insert the battery,
2. place the phone on a flat surface
3. hold the softkeys (1) and (2) while pressing briefly the power button (1 sec)
4. wait till the screen becomes dark, then release the softkeys simultaneously
5. press 0

Now the re-initialization process takes place and the phone will boot up again after a while.

Note: no key material that might compromise the security of your past calls is stored anywhere on your device. Upon completion of a secure call, all key material for the call is destroyed and permanently erased. The recommendation for a Cold Boot in emergency situations only relates to other data stored on the device like notes, contacts, SMS, call history etc.

(like most GSM carriers in the USA), you can switch to the V.32 bearer mode.

To switch the calltype, go the home screen, press the Start softkey and then More --> More --> Configurations --> CSD Line Type (you can also type the keys Start --> 9942 to get there, under most circumstances) . You will get to the configuration menu for CSD data call settings. Now switch the entry under “Data rate” to “9600 bps(V.32). Press the OK softkey. Switch the phone off and on again. To switch back to V.110, use the same menu to change the “Data rate” entry to “9600 bps(V.110)”, press OK and restart the phone by switching it off and on again.

A small desktop phone icon in the CryptoPhone screen will show up if V.32 is activated. The call setup with V.32 takes longer then with V.110, as the modems need some time to synchronize. Incoming calls are not affected by the call type settings.

Problems with setting up a Secure Call

Some providers restrict the reception of GSM data calls, such as needed for the CryptoPhone. The practice is becoming increasingly rare, but a GSM-provider may only allow incoming data calls to subscribers that have

a special 'data subscription', which comes with a special second phone number to call to reach the CryptoPhone. Some providers may not recognize that a number you are calling is a GSM/ISDN number, and erroneously try to handle the call via a modem. This can be recognized by the called party because he/she hears a modem sound when picking up the phone. Some providers may not pass data calls to certain other providers at all.

Under certain circumstances, especially when roaming in GSM networks that are not properly configured, the "never ending key setup" problem may occur. The phenomenon is that the key setup phase takes longer then 20 seconds and never comes to an end. The underlying technical problem resides in the GSM network. Data calls are sometimes set up but then fail to transport any data.

All of the above conditions may make it impossible to use the CryptoPhone in one or both directions between two CryptoPhones. To by-pass this problem if you are roaming try switching providers. If secure calling only works in one direction, you could use an unencrypted call to tell the other party to call you using CryptoPhone. These problems are inherent to using the CSD data call facility and apply to all encrypted telephony over GSM.

General Mobile Phone Security Advice

The use of mobile phones and other radio transmission equipment in certain areas is prohibited or restricted. Because of the risk of interference with life-support equipment, the use of mobile phones is also banned in most hospitals. Using a mobile phone in an airplane is a felony in most countries. You are responsible for complying with local laws and regulations.

Power down

Simply press the power button for three seconds and the phone switches off. The GSMK CryptoPhone firmware is unaffected by a power-down as it resides in non-volatile memory. It is recommended to store the CryptoPhone with the battery removed if it is not used for prolonged periods of time (e.g. several weeks).

Cold Boot & Emergency Erase

Initiating a Cold Boot is recommended in emergency situations, to erase data stored in volatile memory that might compromise your security (like SMS, call history, notes, appointments etc.). Please note that this is not a very secure erasure procedure. Traces of your data might be reconstructed in memory by a skilled adver-

Note: In many countries the use of mobile phones while driving is regulated or completely prohibited. You are responsible for complying with local laws and regulations on telephone use while driving a car. We strongly recommend the use of the enclosed headset while driving, even if local regulations may not require this.

Redialing

The CryptoPhone has access to a call history comprising the last 10 outgoing calls.. You can redial a number by scrolling through the last dialed numbers by moving the joystick up/down and press the green Talk button once the desired number is shown in the display.

Calling from the Contacts list

To call a contact stored in the contact list, press the right soft key in the home screen labeled Contacts. Now you see the list of contacts stored on your SIM and on the phone. The left softkey is now labeled Call Secure. To place the secure call, move the selection bar with the joystick to the contact and press the Call Secure key. The CryptoPhone G10 now switches to the secure call mode and immediately dials the selected contact number in secure mode.

For customers in Europe, North Africa and Asia who experience such problems we recommend our CryptoPhone 200 T/TS solution that uses the Thuraya satellite system to provide the added benefit of affordable secure communication outside GSM covered areas.

Sometimes a specific condition of the GSM network may lead to an unstable state of the GSM part of the CryptoPhone, which also might cause the “never ending key setup”-problem or other undesired behavior. This condition can sometimes be fixed by restarting the CryptoPhone.

Changing the volume

To change the audio volume during a Secure Call, use the volume control buttons on the left side of the device. A volume indicator is located in the lower left corner of the screen and will provide you with visual feedback regarding the volume you set. Please not that the volume levels above green on the indicator (yellow, red) are only designed to be used with a headset or the Push to Talk mode. Chosing them while not using a headset or Push to Talk may lead to distortions and feedback effects that can reduce your call quality considerably.

Mute during call

To mute the microphone during a call, press the softkey labeled “Mute”. To switch the microphone back on again, press the “Mute” key again. The current status is shown in the display with the Mute/Unmute Icon.

Secure Push to Talk

In certain situations, especially when you have a lot of background noise or need a high speaker volume, you can activate the Push to Talk mode (or PTT for short), to achieve good call results. This can be done either during a Secure Call or before. To activate or deactivate PTT, press the “Menu” Softkey, choose “Push to Talk” in the Settings screen, toggle the setting with the center click and press the Done softkey to return to the main screen. PTT works like a two-way radio. When you want to talk, you press the PTT button. When you finshed speaking, you release the button. The button used for PTT on your CryptoPhone G10 is the Camera button on the right side of the device. Please do not forget to release the talk button when you finished talking.

Secure Calls while moving

When using the GSMK CryptoPhone while moving fast in a car or a train, you may experience a degradation in call sound quality, periods of longer delay and short dropouts during a call. These effects are the result of a so called handover that occurs when you move from the coverage zone of one GSM tower (also called 'GSM cell') to the next. During the handover the data connection is briefly interrupted. To prevent important call contents from getting lost, the GSMK CryptoPhone, unlike other encrypted voice systems, accelerates the speed of decoding for a moment after the dropout, to catch up with the lost transmission time. This results in the voice of your partner rising in pitch (the »Mickey Mouse effect«) for a moment. After a short time the pitch returns to normal. The GSMK CryptoPhone G10 has been successfully tested traveling at speeds of up to 180km/h. The frequency and intensity of disturbances is primarily determined by the GSM network. In rural areas, the network consists of fewer and bigger cells, resulting in less frequent handovers and less disturbances. In urban areas the network has typically a high density of small cells, resulting in many handovers when moving and thereby causing more disturbances.